AMENDMENTS TO THE SPECIFICATION

Please amend paragraph [0002] on page 1 as follows:

[0002] Recently, an increasing number of multi-user electronic devices have been produced, and a plurality of users can now simultaneously use ~~one~~ the same device. For example, a user A can access a device owned by the user A using a terminal, and another user B can also access the device owned by the user A.

Please amend paragraph [0003] on page 1 as follows:

[0003] In the case where a user lends a device to another individual via a network, security is the most important issue. For example, in the case where a device is physically lent, the users transfer the device hand to hand, so that the users can manage who will use the device. However, in the case where an access is permitted to an electronic device storing a resource (hereinafter, referred to as a "resource providing device") from another electronic device (hereinafter, referred to as a "resource use device") via a network such that the resource use device can use a function of the resource providing use device, there is a possibility that the resource providing device ~~is~~ will be illegally accessed by a third party without the knowledge of the owner of the resource providing device.

Please amend paragraph [0004] on page 2 as follows:

[0004] Non-patent document 1 describes a protocol for solving this problem (hereinafter, referred to as a "UPnP (Universal Plug and Play) security"). The UPnP security is a general-purpose protocol for allowing a control-side electronic device (hereinafter, referred to as an "access control device"), for controlling the use of a resource by a resource use device, to control

a resource providing device via a network. Use of the UPnP security allows ~~accesses~~ access from the resource use device to the resource providing device to be controlled.

Please amend paragraph [0006] on page 2 as follows:

[0006] However, with the UPnP security, an unnecessary access permission cannot be quickly discarded unless a validity period is set when the access permission is given. An unnecessary access permission should be discarded, and the duration from the time when the access permission ~~comes to a state to~~should be discarded until the access permission is actually discarded should be as close to zero as possible ~~to zero~~.

Please amend paragraph [0008] on page 3 as follows:

[0008] The conventional communication system described in patent document 1 stops the use of all the electronic devices belonging to the group when the existence of even one electronic device cannot be confirmed. This may limit ~~an~~ access even from an electronic device belonging to the group, the existence of which can be confirmed, and does not discard the access permission of only the electronic ~~device, the access permission given to~~device which should be discarded.

Please amend paragraph [0011] on page 4 as follows:

[0011] According to the present invention, when communication with the resource use device is disconnected, the access control device instructs the resource providing device to reject an access from the resource use device. Thus, ~~an~~ illegal access from the resource use device to the resource providing ~~device, an access permission given to which should be discarded,~~ device can be prevented when access permission previously given should be discarded.

Please amend paragraph [0013] on page 5 as follows:

[0013] For example, the information on the resource use device may be information for identifying the resource use device, or may include information for identifying the resource use device and information for identifying the resource providing device for accepting an access from the resource use device. In the case where the information on the resource use device includes information for identifying the resource providing device, the resource providing device to be accessed by the resource use device can be quickly specified.

Please amend paragraph [0015] on page 5 as follows:

[0015] The access permission unit may notify the resource providing device of the information on the resource use device to be permitted to ~~aecess,~~access via the communication unit. Thus, the resource providing device can quickly specify the resource use device which should be permitted to access.

Please amend the sub-heading on page 12, line 9 as follows:

~~BEST MODE FOR CARRYING OUT~~DETAILED DESCRIPTION OF THE INVENTION

Please amend paragraph [0036] on page 14 as follows:

[0036] The resource use device 30 temporarily accesses the resource providing device 20 to use a resource of the resource providing device 20. Herein, the expression "use a resource" means that the resource use device 30 access the resource providing device 20 and uses a part of, or the entirety of, the functions of the ~~aecess~~ resource providing device 20. For example, the resource use device 30 accesses data stored in the resource providing device 20, or inputs data to,

or outputs data from, a device implemented by the resource providing device 20.

Please amend paragraph [0043] on page 17 as follows:

[0043] In the access 14, information on a resource to be accessed by the resource use device 30, among the resources stored in the resource providing device 20, is recorded. Specifically, a command usable by the resource use device 30 and information regarding a parameter for the command (hereinafter, referred to as a "parameter restriction") are recorded in the access 14. In the example shown in ~~FIG. 6~~FIG. 2, functions realized by a combination of a command and information regarding a parameter restriction are shown for better understanding.

Please amend paragraph [0050] on page 19 as follows:

[0050] In the access 23, information on the resource to be accessed by the resource use device 30, among the resources stored in the resource providing device 20, is recorded. Specifically, a command usable by the resource use device 30 and information regarding a parameter for the command are recorded in the ~~access 14~~access 23. Upon receiving a command from the resource use device 30, the resource providing device 20 refers to the access management table 204 to determine whether or not to permit an access from the resource use device 30 based on the access 23 corresponding to the use side 22.

Please amend paragraph [0054] on page 20 as follows:

[0054] The access permission unit 106 receives information on the resource use device 30 which is to access the resource providing device 20 from an input unit (not shown) of the access control device 10, and records the information in the permission information management table 104. The information on the resource use device 30 may be input by the user via the input unit of

the access control device 10, or may be transmitted from the ~~access~~ resource use device 30. Alternatively, information on the resource use device 30 may be stored in the storage unit 103 of the access control device 10 beforehand, and relevant information may be selected and input.

Please amend paragraph [0060] on page 22 as follows:

[0060] The existence check unit 107 determines whether or not the resource use device 30 recorded in the permission information management table 104 exists in the network. Specifically, the existence check unit 107 generates an existence check instruction and transfers the instruction to the communication unit 101. The existence check unit 107 then receives a response transmitted from the resource use device 30 via the communication unit 101 and thus confirms the existence of the resource use device 30. When the existence of the resource use device 30 cannot be confirmed, i.e., when the response from the resource use device 30 is not received, the existence check ~~unit 206~~ unit 107 notifies the access discard ~~unit 207~~ unit 108 of the device ID of the resource use device 30.

Please amend paragraph [0073] on page 28 as follows:

[0073] The communication unit 201 is an interface with the network, and transfers an instruction received from the network to the existence check unit 206, the access discard unit, or the resource access permission unit 205. Upon receiving a response from the existence check instruction, the communication unit 201 transfers the response to the existence check unit 206. Upon receiving an access permission discard instruction, the communication unit 201 transfers the access permission discard instruction to the access discard unit 207. Upon receiving an access instruction, the communication unit 201 transfers the access instruction to the resource access permission unit 205. Upon receiving an instruction to be transmitted from the access

discard unit 207 or the existence check unit 205, the communication ~~unit 101~~unit 201 transmits the instruction to the network.

Please amend paragraph [0079] on page 30 as follows:

[0079] In order to control the use of the resource by the resource use device 30, the access control device 10 and the resource providing device 20 make a preparation. For example, the access control device 10 and the resource providing device 20 establish a mutually communicable state via a communication path (in this example, connection 40). For this, any known method is usable. For example, each device automatically may recognize that the device is connected to the network and obtain information necessary for the connection including such as an IP address or the like using the UPnP technology described in non-patent document 1, and then a mutually communicable state may be established. The user may directly input information necessary for the connection via an input unit (not shown) of each device. Referring to ~~FIG. 2~~FIG. 8, the sequence will be described with an assumption that the preparation is already made and the resource providing device 20 has authenticated an instruction from the access control device 10 and recognizes that an access from the resource use device 30 is permitted.

Please amend paragraph [0083] on page 31 as follows:

[0083] After transmitting the access permission notification instruction, the access control device 10 checks the existence of the resource use device 30 at a predetermined time interval (step S104). When the existence of the resource use device 30 can be confirmed (step S105), the access control device 10 does not generate an access discard instruction.

Please amend paragraph [0084] on page 32 as follows:

[0084] After steps S101 and S102, the resource use device 30 generates an access instruction for accessing the ~~access~~ resource providing device 20 storing a resource, an access to which needs to be controlled, and transmits the instruction to the resource providing device 20 (step S106). Upon receiving the access instruction, the resource providing device 20 refers to the access management table 204 to determine whether or not to permit an access. Specifically, the resource providing device 20 determines whether or not the command and the device ID recorded in the received access instruction match the command and the device ID recorded in the access management table 204. Only when the commands and the device IDs match each other, the resource providing device 20 permits an access. Thus, processing in accordance with the command is executed, and the resource use device 30 is allowed to use the resource.

Please amend paragraph [0103] on page 37 as follows:

[0103] The access control device 10 checks the existence of the resource use devices 30 having the devices ID recorded in the use side 12 in accordance with the order recorded in the permission information management table 104. For checking the existence of the resource use devices 30 recorded in the permission information management table 104, the access control device 10 also communicates using the communication ~~interface 102~~interface 13 associated with the device ID of each resource use device 30.

Please amend paragraph [0110] on page 39 as follows:

[0110] First, in the resource providing device 20, the resource access permission unit 205 receives an access permission instruction transmitted from the access control device 10 via the communication unit 201 (step S31), and updates the access management table 204. Specifically, the resource access permission unit 205 refers to the access management table 204 to record the device ID corresponding to the resource use device 30 recorded in the access permission instruction and also record the control information recorded in the access permission instruction, in the ~~access 201~~access 23.

Please amend paragraph [0123] on page 43 as follows:

[0123] When communication between the resource providing device and the access control device is disconnected, the access control device cannot transmit an access permission discard instruction to the resource providing device. When this occurs, it is desirable from the viewpoint of security that the resource providing device discards access control on the ~~access~~ resource use device which is accessing to the resource providing device.

Please amend paragraph [0124] on page 44 as follows:

[0124] In this case also, according to this embodiment, when the existence of the access control device cannot be confirmed, the resource providing device deletes the information on the access control device, the existence of which cannot be confirmed, and on the resource use device controlled by such an access control device, from the access management table. After this, the resource providing device rejects an access from the resource use device, the information of which has been deleted from the access management table. Thus, even when an access permission discard instruction cannot be transmitted from the access control device, unnecessary

access permissions can be quickly discarded and illegal ~~accesses~~ access to the resource providing device using the resource use device can be prevented. Therefore, the confidentiality of the system can be further improved.

Please amend paragraph [0132] on page 47 as follows:

[0132] Hereinafter, specific examples of an operation of the access control system described in the ~~first~~ above-described embodiment will be described. The present invention is not limited to these examples.

Please amend paragraph [0135] on page 48 as follows:

[0135] While the personal computer in the company B is accessing data in the server, the mobile phone checks the existence of the personal computer at a predetermined time interval using the short distance wireless communication. When Mr. Koh finishes the visit to Mr. Otsu and leaves the company B, the distance between the personal computer and the mobile phone increases. The mobile phone instructs the server to delete the information on the personal computer from the access management table 204 when the connection via the short distance wireless communication is disconnected. Thus, after ~~Mr. A~~Mr. Koh leaves the company B, the access permission from the personal computer to the server can be quickly discarded. Therefore, illegal accesses to the server using the personal computer can be prevented, and the confidentiality of the system can be improved.